

An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review

Pallavi V Chavan¹, Dr. Mohammad Atique², and Dr. Anjali R Mahajan²

¹CE Department, BDCE, Sevagram, India

Pallavichavan11@gmail.com

²PG Department of Computer Science, SGBAU, Amravati, India

Mohd.atique@gmail.com

Abstract—This paper introduces the idea of hierarchical visual cryptography. Authentication is the important issue over the internet. This paper describes a secured authentication mechanism with the help of visual cryptography. Visual cryptography simply divides secret information in to number of parts called shares. These shares are further transmitted over the network and at the receiving end secrets are revealed by superimposition. Many layers of visual cryptography exist in proposed system hence called hierarchical visual cryptography. Remote voting systems now a day's widely using visual cryptography for authentication purpose.

Index Terms— Visual cryptography, secret sharing, shares, authentication.

I. INTRODUCTION

Visual cryptography is the art of encrypting information such as handwritten text, images etc. in such a way that the decryption is possible without any mathematical computations and human visual system is sufficient to decrypt the information. The cryptography scheme is given by the following setup. A secret image consists of a collection of black and white pixels. Here each pixel is treated independently. To encode the secret image, we split the original image into n modified versions (referred as shares) such that each pixel in a share now subdivided into n black and white sub-pixels. To decode the image, a subset S of those n shares are picked and copied on separate transparencies [1]. Visual cryptography schemes were independently introduced by Shamir. Shamir divided data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of $k - 1$ pieces reveals absolutely no information about D . This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces [2]. The first form of visual cryptography is also known as secret sharing.

The simplest form of visual cryptography separates a secret into two parts so that either part by itself conveys no information. When these two parts are combined together by means of superimposition, the original secret can be revealed. These parts are called as shares. There are several advantages of visual cryptography. Basically it is simple to use and no mathematical computations are required to reveal

the secret. Secondly, the individuals who do not have knowledge of cryptography are indirectly getting involved in decryption. The major drawback of this scheme is that visually blind people cannot make use of this technique. The simple example of visual cryptography is shown in Figure1 [3].

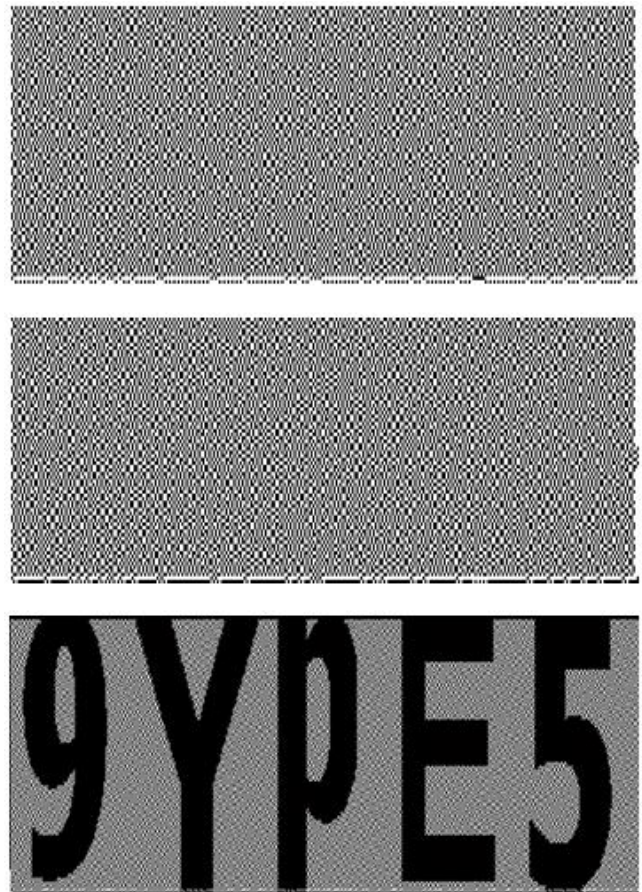


Figure 1. An example of visual cryptography with share 1 , share2 & decoded password

II. LITERATURE REVIEW

There are number of visual cryptography schemes in existence. Some of them are described below.

A. 2 out of 2 Visual Cryptography Scheme

In this type of visual cryptography scheme, the secret image is divided into exactly two shares. This is the simplest kind of visual cryptography. The major application of this

scheme is found with remote voting system that uses 2 out of 2 secret sharing schemes for authentication purpose. To reveal the original image, these two shares are required to be stacked together [4], [5]. Figure 2 represents the division of black and white pixel in this scheme.















| Pixel | White  | | Black  | |
|-------------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Prob. | 50% | 50% | 50% | 50% |
| Share 1 |  |  |  |  |
| Share 2 |  |  |  |  |
| Stack share 1 & 2 |  |  |  |  |

Figure 2. Basic concept of 2 out of 2 scheme

B. K out of N Visual Cryptography

This kind of scheme allows dividing a secret into K number of shares. Then the secret can be revealed from any N number of Shares among K . The major problem associated with this scheme is that the user needs to maintain many shares which may result into loss of shares. Also more number of shares means more memory consumption. The application of this scheme is found with banking system. For the joint accounts, three shares are generated. One is kept with bank's server, second is delivered to the one customer for the joint account and third share is delivered to the second customer. Hence both customers are able to access the account [6].

C. K out of K Visual Cryptography

Here original secret is divided into K number of shares and for reconstruction of the secret, all K shares are necessary. This scheme is not so popular because managing k number of shares is difficult task and it also increases time complexity to compute shares [7].

III. COMPARATIVE ANALYSIS

Research on visual cryptography is still in its infancy. In visual cryptography many schemes are proposed that depends on type of secret to be encrypted and type of share generation approach [18]. Most of the schemes are designed to minimize the memory requirement as well as simplifying the share type i.e. meaningful share or meaningless share. Some of the interesting parameters studied in literature are secret type, number of shares, pixel expansion, type of share etc. Chao Chan and Yi Wu stated a new visual cryptography scheme for secure digital transmission [19],[20]. Visual cryptography can be seen as a one-time pad system which cannot be reused. Authors applied Diffie and Hellman (D-H) key agreement method such that visual cryptography can be

reused. Both secret and symmetry-key are represented in binary image. The proposed scheme was simple and easy to be implemented for shadow images. The shadow images are nothing but the shares. Therefore, it was used in many electronic business applications. The authors also performed security analysis on the implemented scheme.

TABLE I
COMPARISON OF VISUAL CRYPTOGRAPHY SCHEMES

| Authors | Number of Secrets & covers | Pixel expansion | Number of shares | Type of share |
|--------------------------------------------|----------------------------|-----------------|------------------|-------------------|
| Adi Shamir, 1979 | Single secret | Not specified | 2 | Random |
| Chao Chan and Yi Wu, 2008 | Single secret | Not specified | 2 | Random |
| Che Lee and Wen Tsai, 2010 | Single secret and 1 cover | 1:1 | n | Random |
| R. Youmaran and A. Adler, Mini, 2006 | Single secret and 2 covers | 1:4 | 2 | Meaningful shares |
| Chen, Wu and Lee, 2007 | Single secret and 1 cover | 1:4 | 2 | Random |
| Naor and Shamir, 1998 | 1 secret image | 1:4 | 2 | Random |
| D. Jena and S. Jena, 2008 | Single secret and 1 cover | 1:4 | 2 | Random |
| G. Abboud, Marean and Roman, 2010 | Single secret and 1 cover | Not specified | 3 | Random |
| C. Hedge, Shenoy, Venugopal, Patnaik, 2008 | Single secret | Not specified | Multiple | Random |

IV. PROPOSED WORK

In view of above observations and from review of current literatures about various visual cryptography schemes, it is proposed to investigate as follows:

- 1) Analyzing the constraints such as pixel expansion, memory requirement, number of shares, type of share, time complexity while generating shares.
- 2) Innovating new visual cryptography scheme for secured authentication to the intelligent system.
- 3) Multiple secrets encryption in same shares.
- 4) Design and implementation of intelligent system using the approach of hierarchical visual cryptography for the purpose of secured authentication.
- 5) Comparison between proposed and existing authentication techniques in the area of cryptography.

The proposed research is aimed at design and implementation of an intelligent system with secured authentication using hierarchical visual cryptography.

V. CONCLUSIONS

The authentication scheme proposed here is providing security in multiple levels. The share individually is unable to reflect secrecy of the data. The permutations and combinations are failure against the shares. The visual cryptography scheme is also known in the form of secret sharing scheme. Color visual cryptography schemes also exist which is equivalent to steganography concept in network security.

REFERENCES

- [1] Hegde C ,Manu S, Shenoy P D, Venugopal, K. R., Patnaik L. M, "Secured Authentication using Image Processing and Visual Cryptography for Banking Applications," in *Proceedings of 16th IEEE International Conference on Advanced Computing and Communications, ADCOM 2008*, 2008, pp. 65-72.
- [2] Adi Shamir, "How to Share a Secret," in *Communications of ACM*, Vol. 22, no.11, 1979, pp. 612-613.
- [3] Pallavi V. Chavan, R.S. Mangrulkar, "Sharing a Secret in Network," in *International Engineering and Technology Journal of Information System*, Vol.4, no. 2, pp.83-87.
- [4] Zhongnin Wangarce, G.R., "Halftone Visual Cryptography by Interactive Halftoning," in *Proceedings of 2010 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, March 2010, pp. 1822-1825.
- [5] Moni Naor, Adi Shamir, "Visual Cryptography," in *Springer-Verlag International Journal*, 1998, pp. 1-11.
- [6] Tzung, Chang Sain, Wei Lee, "A Novel Subliminal Channel Found in Visual Cryptography and Its Application to Image Hiding," in *Proceedings of 3rd IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Vol. 1, 2007, pp. 421-424.
- [7] Che Lee, Wen Tsai, "Authentication of Binary Images in PNG Format Based on a Secret Sharing Technique," in *Proceedings of IEEE International Conference on System and Engineering, Taipei*, July 2010, pp. 506-510.
- [8] R. Youmaran, A. Adler, A. Miri, "An Improved Visual Cryptography Scheme for Secret Hiding," in *Proceedings of 23rd IEEE Biennial Symposium on Communications*, 2006, pp. 340-343.
- [9] P. S. Revenkar, Anisa Anjum, W. Gandhare, "Survey of Visual Cryptography Schemes," *International Journal of Security and Its Applications*, Vol. 4, no. 2, April 2010, pp. 49-56.
- [10] Bin Yu, Jin Lu, Li Fang, "A Co-Cheating Prevention Visual Cryptography Scheme," in *Proceeding of 3rd IEEE International Conference on Information and Computing*, 2010, pp.157-160.
- [11] Ayesha Altaf, Rabia, Attiq, "A Novel Approach against DoS Attacks in WiMAX Authentication using Visual Cryptography," in *Proceedings of IEEE International Conference on Emerging Security Information, Systems and Technologies*, 2008, pp. 238-242.
- [12] Jena D, Jena S. K., "A Novel Visual Cryptography Scheme," in *Proceedings of IEEE International Conference on Advanced Computer Control*, 2009, pp. 207-211.
- [13] Abboud, G., Marean, J., Yampolskiy, R.V., "Steganography and Visual Cryptography in Computer Forensics," in *Proceedings of 5th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2010, pp. 25-32.
- [14] Shang Chen, Sian Lin, "Non expansible flip-flop visual cryptography with perfect security," in *Proceeding of 5th IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2009, pp.949-952.
- [15] Jonathan and Wei Yan, "Image Hatching for Visual Cryptography," in *Proceeding of 13th IEEE International Conference on Machine Vision and Image Processing*, 2009, pp. 59-64.
- [16] Abboud, G., Marean, J. and Yampolskiy, R.V., "Steganography and Visual Cryptography in Computer Forensics," in *Proceeding of 5th IEEE International Workshop on Systematic Approaches to Digital Forensics Engineering*, 2010, pp. 25-32.
- [17] Weir, Yan, "Sharing Multiple Secretes using Visual Cryptography," in *Proceeding of IEEE International Symposium on Circuits and Systems*, 2009, pp. 509-512.
- [18] Chao Wen, Yi Wu, "A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme," *International Journal of Computer Science and Network Security*, Vol. 8, no. 4, April 2008, pp. 128-132.
- [19] Li Fang, Ya-Min Li, Bin Yu, "Multi Secret Visual Cryptography based on Reversed Images," in *Proceeding of 3rd IEEE International Conference on Information and Computing*, 2010, pp. 195-198.
- [20] Thomas Monoth, Babu Anto P, "Contrast Enhanced Visual Cryptography Schemes based on Additional Pixel Pattern," in *Proceeding of IEEE International Conference on Cyberworlds*, 2010, pp. 171-178.